NIST and NSTB Assess Use of Antivirus Software on Industrial Control Systems

NIST and NSTB staff at Sandia National Laboratories investigated and tested the impacts of commercial, off-the-shelf antivirus software on industrial control system (ICS) performance. The results are available in *Using Host-Based Antivirus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts*. This publication provides the industrial control systems community with useful information on ICS security, guidance and practices for minimizing adverse impacts of anti-virus software on time-critical processes. In addition, it offers a methodology for developing custom test procedures to assess performance impacts. The document is designed as a secondary resource for use when installing, configuring, running or maintaining antivirus software on an ICS.

Major findings from the laboratory tests, as summarized below, tend to support industry feedback:

- Manual or "on-demand" scanning has a major effect on control processes in that they take CPU time needed by the control process (Sometimes close to 100% of CPU time). Minimizing the antivirus software throttle setting will reduce but not eliminate this effect.
- Active scanning or "on-access" scanning has little or no effect on control processes.
- Signature updates can also take up to 100% of CPU time, but for a much shorter period than a typical manual scanning process.

In many cases, performance impacts can be reduced by using different configuration settings, scanning practices and maintenance scheduling than those recommended for typical IT system applications. Control system vendors typically specify antivirus software configuration settings for use with their own line of products.

This document was made possible through the support of eleven industry partners who hosted site visits or provided guidance. The results address one of the industry-defined priorities in the *Roadmap To Secure Control Systems in the Energy Sector* pertaining to the use on antivirus software with control systems: Disseminate field-proven best practices for control system security. The working relationships established with the antivirus software vendors participating in this project lay the groundwork for achieving another: Develop cost-effective antivirus protection that minimizes host impact.

The National SCADA Test Bed is a multi-laboratory partnership providing integrated expertise to identify and correct critical security flaws in control systems and equipment. The NSTB team is jointly led by Idaho National Laboratory and Sandia National Laboratories. It operates under the auspices of the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability, which leads national efforts to modernize the electric grid, enhance the security and reliability of the energy infrastructure, and facilitate recovery from disruptions to energy supply.

Contact: Joe Falco at falco@cme.nist.gov